Caching UAV Assisted Secure Transmission in Hyper-Dense Networks Based on Interference Alignment

Nan Zhao, *Senior Member, IEEE,* Fen Cheng, F. Richard Yu, *Senior Member, IEEE,* Jie Tang, *Member, IEEE,* Yunfei Chen, *Senior Member, IEEE,* Guan Gui, *Member, IEEE,* and Hikmet Sari, *Fellow, IEEE*

***Abstract*—Unmanned aerial vehicles (UAVs) can help small-cell base stations (SBSs) offload traffic via wireless backhaul to improve coverage and increase rate. However, the capacity of backhaul is limited. In this paper, UAV assisted secure transmission for scalable videos in hyper-dense networks via caching is studied. In the proposed scheme, UAVs can act as SBSs to provide videos to mobile users in some small cells. To reduce the pressure of wireless backhaul, UAVs and SBSs are both equipped with caches to store videos at off-peak time. To facilitate UAVs, a single antenna is equipped at each UAV and thus, only the precoding matrices of SBSs should be cooperatively designed to manage interference by exploiting the principle of interference alignment. On the other hand, the SBSs replaced by UAVs will be idle. Thus, in order to guarantee secure transmission, the idle SBSs can be further exploited to generate jamming signal to disrupt eavesdropping. The jamming signal is zero-forced at the legitimate users through the precoding of the idle SBSs, without affecting the legitimate transmission. The feasibility conditions of the proposed scheme are derived, and the secrecy performance is analyzed. Finally, simulation results are presented to verify the effectiveness of the proposed scheme.**

***Index Terms*—Caching, interference alignment, physical layer security, small-cell networks, unmanned aerial vehicles.**

I. Introduction

In 5G mobile networks, data traffic will increase unprecedentedly. In order to meet the increasing data demands, small-cell networks will be widely deployed, which can achieve much higher throughput and energy efficiency [1]. However, owing to the dense deployment of small-cell base stations (SBSs), the interference between users becomes more serious, which may lead to performance degradation. Thus, it is very important to properly manage interference to further improve the performance of small-cell networks [2]. As an emerging technique for interference management in wireless networks, interference alignment (IA) can be utilized in hyder-dense small-cell networks [3]–[8]. In addition, the security of small-cell networks is also a critical issue, which has attracted significant attention [9]–[14].

To alleviate the pressure of small cells and reduce the cost of densely deployed SBSs, unmanned aerial vehicles (UAVs) can be exploited to assist small cells in providing high-speed transmission due to their low cost and high mobility. UAV-aided wireless networks can establish wireless connections without infrastructure, realize larger wireless coverage, and achieve higher transmission rate. Thus, a number of research works on this topic have been done in recent years [15]–[22]. In [15], three typical cases of utilization for UAV-aided wireless communications were summarized by Zeng *et al*., including UAV-aided ubiquitous coverage, UAV-aided relaying, and UAV-aided information dissemination. In [16], Gupta *et al*. discussed the key issues of routing and protocol in UAV-aided communications. A sub-modular game perspective of energy consumption optimization of UAV-aided network was provided in [17] by Koulali *et al*. In [18], Sharma *et al*. proposed a user demand based network model to achieve prolonged connectivity, bigger capacity and better reliability in heterogeneous networks assisted by UAVs. In [19], a spiral algorithm was proposed by Lyu *et al*. to minimize the number of required UAV-mounted mobile base stations to cover all the ground terminals. Zeng *et al*. optimized the throughput for UAV-aided mobile relaying system by transmitting appropriate source/relay power along with selecting appropriate relay trajectory in [20]. While in [21], energy-efficient network was achieved through optimizing the UAV's trajectory by Zeng and Zhang. In addition, in small-cell networks, UAVs can serve as mobile base stations to assist SBSs in offloading data traffic via wireless backhaul [22].

However, UAVs can provide data transmission only by connecting to the macro-cell base station (MBS) via wireless backhaul. Due to the limited capacity of wireless backhaul, the transmission rate by UAVs is also limited, which will degrade the quality of service (QoS) when mobile users are crowded. To solve this problem, caches can be equipped at UAVs to store the popular contents at off-peak period [23], and thus, when the users' requested contents exist at local caches of UAVs, they can be delivered to the users directly without wireless backhaul at peak period. Thus, the load via limited wireless backhaul can be reduced, which makes UAVs more feasible.

In cache-aided wireless networks, the local caches proactively fetch the popular files from the core network during off-peak time [24]–[27], and the users can obtain the required contents from the edge nodes directly at peak time, e.g., SBSs, instead of the core network. Thus, the traffic at the backhaul can be shifted from the peak time to the off-

N. Zhao and F. Cheng are with the School of Inform. and Commun. Eng., Dalian University of Technology, Dalian, Liaoning, P. R. China (email: zhaonan@dlut.edu.cn, 251791@mail.dlut.edu.cn).

F.R. Yu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, K1S 5B6, Canada (email: richard.yu@carleton.ca).

J. Tang is with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, Guangdong, P. R. China (Email: eejtang@scut.edu.cn).

Y. Chen is with the School of Engineering, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: Yunfei.Chen@warwick.ac.uk).

G. Gui is with Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, P. R. China (e-mail: guiguan@njupt.edu.cn).

H. Sari is with Sequans Communications, 92700 Colombes, France. He is also with Department of Telecommunication, CentraleSupelec, 91192 Gif-sur-Yvette France (email: hikmet.sari@supelec.fr).

peak time, and the pressure of backhaul will be significantly relieved [28]. In addition, caching at the edge of networks makes the data traffic much closer to the mobile users. Thus, the transmission latency can be reduced, and the quality of experience for users will be enhanced. Furthermore, caching can also be utilized in interference networks, especially, IA-based networks, to facilitate the interference management and improve the performance [7], [8], [29], [30]. In [29], each file was divided into some nonoverlapping subfiles cached at different transmitters, and then, those subfiles would be transmitted to users cooperatively by managing interference effectively with IA gain. Deghel *et al*. demonstrated that caching can provide benefits for IA networks in [30]. In [7], caching and computing were jointly utilized by Zhao *et al*., to simplify the topology of IA networks, reduce backhaul load, and thus improve the throughput. In [8], power allocation was researched by Cheng *et al*. in cached-aided small-cell networks with limited backhaul.

Motivated by the above works, in this paper, UAVs with caching are utilized as mobile base stations (BSs) to provide video streaming to the mobile users along with SBSs. To effectively eliminate the interference between users, IA is exploited in the proposed scheme. In addition, to guarantee the secure transmission, the idle SBSs replaced by UAVs are further utilized to generate jamming signal to disrupt the potential eavesdropping, without affecting the legitimate transmission. The key contributions of this paper can be summarized as follows.

- To the best of our knowledge, there are very few works on UAV-aided wireless networks with caching [23]. Thus, in this paper, we propose a comprehensive framework for hyper-dense small-cell networks assisted by caching UAVs, analyze its feasibility, and discuss the secure transmission.
- To relieve the transmission pressure of SBSs, UAVs are utilized to provide data traffic to mobile users cooperatively with SBSs, due to their lower cost and higher mobility. Caches are equipped at UAVs to store popular files in advance, which can relieve the pressure on the wireless backhaul at peak time significantly.
- A single antenna is equipped at each UAV to facilitate its transmission, and the idea of IA is leveraged to perform interference management in the network through designing the precoding matrices of SBSs cooperatively. The feasibility conditions of the proposed scheme are also derived.
- Another key issue for the UAV aided small-cell network is the secure transmission. In this paper, the idle SBSs replaced by UAVs are further utilized to generate jamming signal to disrupt the potential eavesdropping, which will not affect the transmission of the legitimate network. The security performance of the proposed scheme is analyzed.

In addition, some issues for adopting IA in our proposed scheme are discussed as follows.

(1) The performance of IA will degrade at low SNRs, due to the fact that it only concentrates on interference, instead of noise. First, to make it more practical to be utilized at low SNRs, plenty of research has been done to improve its performance [31]–[34]. In addition, although the performance of IA is not optimal at low SNRs, it will instruct the optimal transceiver design of MIMO interference network, according to its feasibility conditions [35], i.e., the optimal MIMO transceiver design scheme can achieve reliable performance only when the feasibility conditions of IA can be satisfied. Last, although we adopt IA to achieve interference management in this manuscript, the framework can also be achieved by other interference management techniques, e.g., optimal transceiver design [36].

(2) Channel state information (CSI) estimation errors will degrade the performance IA obviously. Nevertheless, there have been a lot of research efforts focusing on this aspect [6], [37]–[39], e.g., CSI overhead reduction, limited quantization, channel prediction, blind IA, *etc*. These achievements can be further combined with our proposed scheme to overcome the CSI problem, which is not the main task of this paper. In addition, only one single antenna is equipped at each UAV, which does not need the CSI knowledge. Thus, the challenge for the estimation of CSI for mobile UAVs can be avoided.

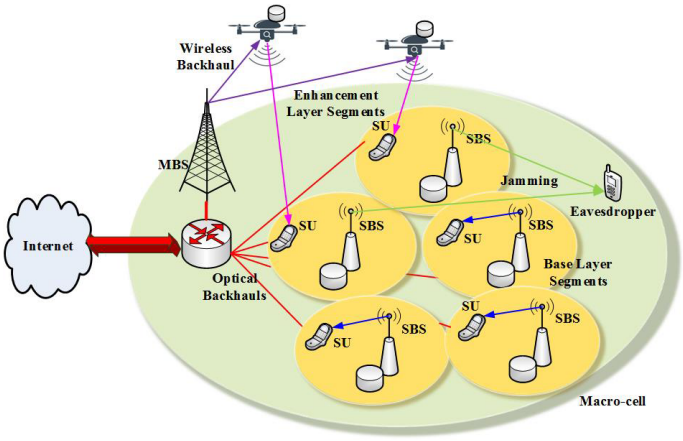

Fig. 1. UAV assisted secure transmission in hyper-dense networks via caching.

The rest of this paper is organized as follows. In Section II, the system model is described. In Section III, the interference management scheme for the caching UAV assisted hyper-dense network with jamming signal is proposed, and its feasibility conditions are derived in Section IV. In Section V, the security performance of the proposed scheme when there exists an eavesdropper is analyzed. Simulation results are presented in Section VI, followed by conclusions and future work in Section VII.

Notation: $\mathbf{A}^{\dagger}$ is the conjugate transpose of matrix $\mathbf{A}$. $\mathbf{I}_N$ represents $N \times N$ indentity matrix. $\mathcal{CN}(\mathbf{a}, \mathbf{A})$ represents the complex Gaussian distribution with mean $\mathbf{a}$ and covariance matrix $\mathbf{A}$. $\mathbf{v}_i(\mathbf{A})$ and $\mathbf{A}_{\star l}$ are the eigenvector corresponding to the ith smallest eigenvalue and the lth column of matrix $\mathbf{A}$, respectively.

II. System Model

Consider a UAV-assisted hyper-dense small-cell network via caching, as shown in Fig. 1, in which one MBS, K SBSs and

K corresponding mobile users, operate in a specific frequency band[1]. The MBS is connected to the core network via optical backhaul. In addition, there exist A $(A < K)$ UAVs served as mobile BSs, which are connected to the MBS via wireless backhaul to alleviate the data transmission load of SBSs and achieve higher transmission rate. However, due to limited batteries, limited wireless backhaul and high mobility, some special properties of UAVs are considered in the network as follows.

- Only one single antenna is equipped at each UAV[2], due to the fact that the scattering in UAV environment is inadequate, the size, weight and power of UAVs are limited, and CSI cannot be obtained easily at UAVs [15].
- According to the DoF requirement of multi-input and multi-output (MIMO) system, only one data stream can be transmitted by the UAV owing to the single antenna.
- UAVs do not need the CSI knowledge, due to the fact that no precoding is needed with single antenna.
- Caches are equipped at UAVs in order to alleviate the load of wireless backhaul and save energy. Popular videos can be proactively cached at UAVs during off-peak period or when replenishing batteries on the ground.
- Rotary wing UAVs are adopted, which can stay stationary in the air when offloading data, and the transmit power of UAVs cannot be neglected due to the limited batteries, especially when they are far from terrestrial users. Thus, UAVs should fly close enough to the corresponding users when offloading.

To make the caching of videos at UAVs and SBSs more effective, a special video caching strategy is adopted. In this strategy, each video file is divided into two layers, i.e., base layer (BL) and enhancement layer (EL) [40]. When a user requires standard-definition video streaming, only the BL segment of the video file should be transmitted. When the user need high-definition video streaming, both the EL and BL segments should be delivered. To reduce the load and save caching resource, only EL segments are cached at UAVs, while at SBSs, both BL and EL segments are cached. The SBSs can support the BL transmission, and the UAVs only help to offload data traffic when high-definition video streaming is required. Assume that only one layer of the video can be transmitted to each user within each time slot, and thus, at a specific time slot, UAVs can replace SBSs to serve the corresponding users with EL segments in some of the small cells. In this paper, we only consider a special scenario for video streaming transmission. Actually, we can easily extend our proposed scheme to some more general cases when the SBSs and UAVs have cached totally different contents.

Without loss of generality, we assume that the 1st user to the Ath user require EL segments from their corresponding UAVs, and the remaining $(K-A)$ users want to obtain BL segments from their corresponding $(K-A)$ SBSs at a specific time slot.

[1]We assume that only one active user exists in a certain frequency band of each small cell. Nevertheless, more users can be accommodated by orthogonal frequency-division multiple access or other ways, which is beyond the scope of this paper.

[2]The proposed scheme can be easily extended to the case when each UAV is also equipped with multiple antennas.

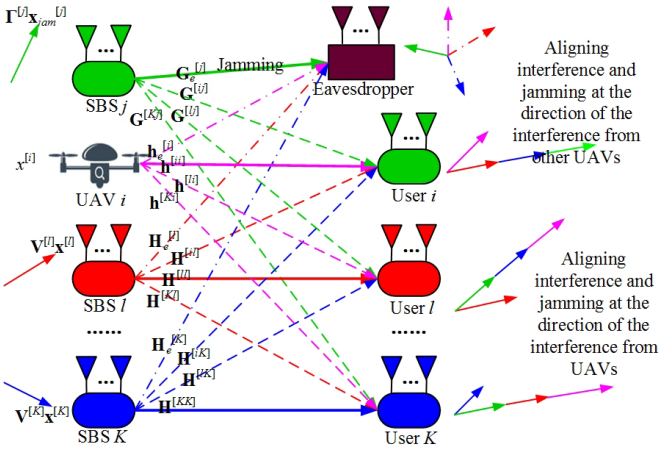

Fig. 2. Interference management for UAV assisted small-cell networks with jamming signal.

Thus, the 1st to the Ath SBSs are idle at the time slot. To fully utilize the resource and guarantee secure transmission, these A SBSs are utilized to generate jamming signal to disrupt potential eavesdropping, without affecting legitimate transmission. Besides, we assume that M_{jam} antennas are active at each jamming SBS. For the remaining lth SBS, M antennas are active, and d independent data streams are transmitted to its corresponding user, $l = A+1, A+2, ..., K$. Each mobile user is equipped with N antennas.

When the transmission is performed in the hyper-dense small-cell network, interference between users may become much more serious. Thus, IA is exploited to effectively manage the interference in the small-cell network, as illustrated in Fig. 2. When IA is performed, no precoding matrices are needed at UAVs as they only have a single antenna. The received signal at the ith user served by UAV can be expressed as

$$\begin{aligned} y^{[i]} =& \mathbf{u}^{[i]\dagger}\mathbf{h}^{[ii]}x^{[i]} + \sum_{a=1,a\neq i}^{A} \mathbf{u}^{[i]\dagger}\mathbf{h}^{[ia]}x^{[a]} \\ &+ \sum_{k=A+1}^{K} \mathbf{u}^{[i]\dagger}\mathbf{H}^{[ik]}\mathbf{V}^{[k]}\mathbf{x}^{[k]} + \mathbf{u}^{[i]\dagger}\mathbf{z}^{[i]}, \end{aligned} \tag{1}$$

where $i = 1, 2, \ldots, A$. $\mathbf{h}^{[ia]}$ is the $N \times 1$ channel coefficient vector between the ath UAV and the ith user, each entity of which is independent and identically distributed (i.i.d.) following $\mathcal{CN}(0,1)$. Similarly, $\mathbf{H}^{[ik]}$ is the $N \times M$ channel coefficient matrix between the kth SBS and the ith user. $\mathbf{V}^{[k]}$ is the $M \times d$ precoding matrix of the kth SBS with $\mathbf{V}^{[k]}\mathbf{V}^{[k]\dagger} = \mathbf{I}_d$. $\mathbf{u}^{[i]}$ is the $N \times 1$ decoding vector of the ith user with $\mathbf{u}^{[i]}\mathbf{u}^{[i]\dagger} = 1$. $x^{[i]}$ is the signal transmitted by the ith UAV with power P_1. $\mathbf{x}^{[k]}$ is the signal vector that consists of d independent data streams with power P_2. $\mathbf{z}^{[i]}$ is the $N \times 1$ additive white Gaussian noise (AWGN) vector with distribution $\mathcal{CN}(\mathbf{0}, \sigma^2 I_N)$ at the ith user, where σ^2 is the noise power at each antenna. The received signal of the lth

user served by SBS can be expressed as

$$\begin{aligned}\mathbf{y}^{[l]} =&\mathbf{U}^{[l]\dagger}\mathbf{H}^{[ll]}\mathbf{V}^{[l]}\mathbf{x}^{[l]}+\sum_{a=1}^{A}\mathbf{U}^{[l]\dagger}\mathbf{h}^{[la]}x^{[a]}\\&+\sum_{\substack{k=A+1\\k\neq l}}^{K}\mathbf{U}^{[l]\dagger}\mathbf{H}^{[lk]}\mathbf{V}^{[k]}\mathbf{x}^{[k]}+\mathbf{U}^{[l]\dagger}\mathbf{z}^{[l]},\end{aligned}\tag{2}$$

where $l = A+1, A+2, \ldots, K$. $\mathbf{U}^{[l]}$ is the $N \times d$ decoding matrix of the lth user, with $\mathbf{U}^{[l]}\mathbf{U}^{[l]\dagger} = \mathbf{I}_d$.

We also assume that there exists a passive eavesdropper with N_e antennas, which tries to eavesdrop the legitimate transmission of the network. The received signal at the eavesdropper without considering the jamming from SBSs can be denoted as

$$\mathbf{y}_e = \sum_{i=1}^{A}\mathbf{h}_e^{[i]}x^{[i]} + \sum_{l=A+1}^{K}\mathbf{H}_e^{[l]}\mathbf{V}^{[l]}\mathbf{x}^{[l]} + \mathbf{z}_e,\tag{3}$$

where $\mathbf{h}_e^{[i]}$ is the $N_e \times 1$ channel coefficient vector between the ith UAV and the eavesdropper. $\mathbf{H}_e^{[l]}$ is the $N_e \times M$ channel coefficient matrix between the lth SBS and the eavesdropper. $\mathbf{z}_e$ is the $N_e \times 1$ AWGN vector with distribution $\mathcal{CN}(\mathbf{0}, \sigma^2 I_{N_e})$ at the eavesdropper.

Remark 1: Despite of the mobility of UAVs, they will stop moving when performing transmission to the users. Thus, IA is suitable to be leveraged in the UAV assisted hyper-dense networks, due to the slow change of CSI.

III. UAV Assisted Hyper-Dense Networks with Jamming Signal

In this section, the interference management scheme is first proposed for the UAV assisted hyper-dense network without jamming signal. Then, the jamming signal is designed without affecting the legitimate transmission. Finally, an algorithm is proposed to fulfill the scheme.

A. Interference Management in the UAV Assisted Network

From Section II, we know that the recovered signal of the mobile user can be expressed as (1) or (2) without considering jamming signal when IA is performed. In order to effectively eliminate the interference between users, the precoding and decoding matrices should be cooperatively designed. In particular, the precoding of UAVs need not be considered due to single antenna equipped. Thus, at the ith user, $i = 1, 2, \ldots, A$, the interference from all the SBSs should be constrained by their precoding matrices into the same subspace of the interference from UAVs. Then, all the interference can be eliminated perfectly using its decoding vector $\mathbf{u}^{[i]}$ to recover the desired signal, based on (4) and (5). Similarly, at the lth user, $l = A+1, A+1, \ldots, K$, the interference from other SBSs should be constrained by the precoding matrices into the same subspace of the interference from UAVs. Then, all the interference can be eliminated perfectly by its decoding matrix $\mathbf{U}^{[l]}$ to recover the desired signal, based on (6) and (7). Therefore, in order to perfectly eliminate the interference between users, the following conditions (4)-(9) should be satisfied for $i = 1, 2, \ldots, A$ and $l = A+1, A+2, \ldots, K$ according to the idea of IA:

$$\mathbf{u}^{[i]\dagger}\mathbf{h}^{[ia]} = 0,\ \forall a = 1, 2, \ldots, A, a \neq i.\tag{4}$$

$$\mathbf{u}^{[i]\dagger}\mathbf{H}^{[ik]}\mathbf{V}^{[k]} = \mathbf{0},\ \forall k = A+1, A+2, \ldots, K.\tag{5}$$

$$\mathbf{U}^{[l]\dagger}\mathbf{h}^{[la]} = \mathbf{0},\ \forall a = 1, 2, \ldots, A.\tag{6}$$

$$\mathbf{U}^{[l]\dagger}\mathbf{H}^{[lk]}\mathbf{V}^{[k]} = \mathbf{0},\ \forall k = A+1, A+2, \ldots, K, k \neq l.\tag{7}$$

$$\mathbf{u}^{[i]\dagger}\mathbf{h}^{[ii]} \neq 0.\tag{8}$$

$$\operatorname{rank}\left(\mathbf{U}^{[l]\dagger}\mathbf{H}^{[ll]}\mathbf{V}^{[l]}\right) = d.\tag{9}$$

When (4)-(7) can be met, the conditions (8) and (9) will be satisfied almost certainly due to the fact that there is not any special structure of the channel matrices. Thus, when (4)-(7) can be solved by the precoding and decoding matrices cooperatively, the proposed scheme will be feasible, and the interference can be perfectly eliminated. The received signal of the ith user served by UAV in (1) can be simplified as

$$y^{[i]} = \overline{h}^{[i]}x^{[i]} + \overline{z}^{[i]},\tag{10}$$

where $i = 1, 2, \ldots, A$, $\overline{h}^{[i]} \triangleq \mathbf{u}^{[i]\dagger}\mathbf{h}^{[ii]}$ and $\overline{z}^{[i]} \triangleq \mathbf{u}^{[i]\dagger}\mathbf{z}^{[i]}$. The received signal of the lth user in (2) can be updated as

$$\mathbf{y}^{[l]} = \overline{\mathbf{H}}^{[l]}\mathbf{x}^{[l]} + \overline{\mathbf{z}}^{[l]},\tag{11}$$

where $l = A+1, A+2, \ldots, K$, $\overline{\mathbf{H}}^{[l]} \triangleq \mathbf{U}^{[l]\dagger}\mathbf{H}^{[ll]}\mathbf{V}^{[l]}$ and $\overline{\mathbf{z}}^{[l]} \triangleq \mathbf{U}^{[l]\dagger}\mathbf{z}^{[l]}$. Thus, the sum rate of the small-cell network can be expressed as

$$R_{sum} = \sum_{i=1}^{A}\log_2\left|1 + \frac{P_1}{\sigma^2}\overline{h}^{[i]}\overline{h}^{[i]\dagger}\right| + \sum_{l=A+1}^{K}\log_2\left|\mathbf{I}_d + \frac{P_2}{d\sigma^2}\overline{\mathbf{H}}^{[l]}\overline{\mathbf{H}}^{[l]\dagger}\right|.\tag{12}$$

B. Design of Jamming Signal

When there exists a potential eavesdropper, the idle SBSs that replaced by UAVs can be further utilized to generate jamming signal to disrupt the eavesdropping. Then, the received signal of the kth user in (10) and (11) can be rewritten as

$$\widehat{y}^{[i]} = \overline{h}^{[i]}x^{[i]} + \sum_{j=1}^{A}\mathbf{u}^{[i]\dagger}\mathbf{G}^{[ij]}\mathbf{\Gamma}^{[j]}\mathbf{x}_{jam}^{[j]} + \overline{z}^{[i]}, i = 1, 2, \ldots, A,\tag{13}$$

$$\widehat{\mathbf{y}}^{[l]} = \overline{\mathbf{H}}^{[l]}\mathbf{x}^{[l]} + \sum_{j=1}^{A}\mathbf{U}^{[l]\dagger}\mathbf{G}^{[lj]}\mathbf{\Gamma}^{[j]}\mathbf{x}_{jam}^{[j]} + \overline{\mathbf{z}}^{[l]}, l = A+1, A+2, \ldots, K,\tag{14}$$

where $j = 1, 2, \ldots, A$, $\mathbf{G}^{[kj]}$ is the $N \times M_{jam}$ channel coefficient matrix between the jth SBS and the kth user, $\mathbf{\Gamma}^{[j]}$ is the $M_{jam} \times d_{jam}$ unitary precoding matrix of the jth SBS, and $\mathbf{x}_{jam}^{[j]}$ is the jamming vector that consists of d_{jam} data streams with transmit power P_{jam}.

From (13) and (14), we can see that the jamming signal will affect the legitimate transmission of the small-cell network, and thus, they should be properly managed. In order to disrupt the eavesdropping without affecting the legitimate transmission, the jamming signal should be perfectly eliminated at the legitimate users. Thus, the following conditions should be

satisfied for $i = 1, 2, \ldots, A$ and $l = A+1, A+2, \ldots, K$ as

$$\mathbf{u}^{[i]\dagger}\mathbf{G}^{[ij]}\mathbf{\Gamma}^{[j]} = \mathbf{0},\ \forall j = 1, 2, \ldots, A, \tag{15}$$

$$\mathbf{U}^{[l]\dagger}\mathbf{G}^{[lj]}\mathbf{\Gamma}^{[j]} = \mathbf{0},\ \forall j = 1, 2, \ldots, A. \tag{16}$$

Based on the interference management scheme in Section III-A, the jamming signal should be constrained in the same subspace of the interference at each legitimate user. In other words, the decoding vectors $\mathbf{u}$ and matrices $\mathbf{U}$ in (15) and (16) have been determined by the conditions (4)-(7) and should not be changed. Thus, only the precoding matrices $\mathbf{\Gamma}$ should be well designed to make (15) and (16) feasible.

When the interference from the undesired transmitters and jamming signal from the idle SBSs can be both perfectly eliminated at each legitimate user, the sum rate of the network is still given by (12).

C. Distributed Algorithm to Achieve the Proposed Scheme

In the proposed scheme, UAVs and SBSs are utilized to provide scalable video segments to their corresponding users. For each mobile user, the interference from other SBSs and UAVs can be eliminated perfectly by IA. In addition, the idle SBSs can be re-utilized to generate jamming signal to disrupt the eavesdropping, which can be perfectly zero-forced at the legitimate users. Thus, a distributed algorithm for UAV assisted hyper-dense networks with jamming signal is proposed, in which the precoding matrices and decoding vectors and matrices can be calculated iteratively. Then, the precoding matrices $\mathbf{\Gamma}$ for jamming can be obtained through zero-forcing.

In the forward direction of iterations, when we consider the interference from other SBSs and UAVs, the interference covariance matrices at the legitimate users can be written as

$$\begin{aligned}\mathbf{Q}^{[i]} = &\sum_{k=A+1}^{K} \frac{P_2}{d}\mathbf{H}^{[ik]}\mathbf{V}^{[k]}\mathbf{V}^{[k]\dagger}\mathbf{H}^{[ik]\dagger} \\ &+ \sum_{a=1, a\neq i}^{A} P_1\mathbf{h}^{[ia]}\mathbf{h}^{[ia]\dagger}, \forall i = 1, 2, \ldots, A.\end{aligned} \tag{17}$$

$$\begin{aligned}\mathbf{Q}^{[l]} = &\sum_{\substack{k=A+1,\\ k\neq l}}^{K} \frac{P_2}{d}\mathbf{H}^{[lk]}\mathbf{V}^{[k]}\mathbf{V}^{[k]\dagger}\mathbf{H}^{[lk]\dagger} \\ &+ \sum_{a=1}^{A} P_1\mathbf{h}^{[la]}\mathbf{h}^{[la]\dagger}, \forall l = A+1, A+2, \ldots, K.\end{aligned} \tag{18}$$

According to (18), $\mathbf{U}_{\star s}^{[l]}$ for the sth data stream at the lth user can be calculated as

$$\mathbf{U}_{\star s}^{[l]} = \mathbf{v}_s(\mathbf{Q}^{[l]}), s = 1, \ldots, d, \tag{19}$$

where $l = A+1, A+2, \ldots, K$. Then, the decoding matrix $\mathbf{U}^{[l]}$ can be obtained by combining the vectors of $\mathbf{U}_{\star s}^{[l]}$. Specially, due to the fact that there is only one data stream transmitted by each UAV, we have

$$\mathbf{u}^{[i]} = \mathbf{v}_1\left(\mathbf{Q}^{[i]}\right), \tag{20}$$

where $i = 1, 2, \ldots, A$.

In the reverse direction, the interference covariance matrices can be computed as

$$\begin{aligned}\overleftarrow{\mathbf{Q}}^{[k]} = &\sum_{i=1}^{A} P_1\overleftarrow{\mathbf{H}}^{[ki]}\overleftarrow{\mathbf{V}}^{[i]}\overleftarrow{\mathbf{V}}^{[i]\dagger}\overleftarrow{\mathbf{H}}^{[ki]\dagger} \\ &+ \sum_{\substack{l=A+1\\ l\neq k}}^{K} \frac{P_2}{d}\overleftarrow{\mathbf{H}}^{[kl]}\overleftarrow{\mathbf{V}}^{[l]}\overleftarrow{\mathbf{V}}^{[l]\dagger}\overleftarrow{\mathbf{H}}^{[kl]\dagger}, \forall k = A+1, A+2, \ldots, K,\end{aligned} \tag{21}$$

where $\overleftarrow{\mathbf{H}}^{[kj]} = \mathbf{H}^{[jk]\dagger}$, $\overleftarrow{\mathbf{v}}^{[i]} = \mathbf{u}^{[i]}$, and $\overleftarrow{\mathbf{V}}^{[l]} = \mathbf{U}^{[l]}$.

According to (21), $\overleftarrow{\mathbf{U}}_{\star s}^{[k]}$ for the sth data stream of the reverse direction can be calculated as

$$\overleftarrow{\mathbf{U}}_{\star s}^{[k]} = \mathbf{v}_s\left(\overleftarrow{\mathbf{Q}}^{[k]}\right), s = 1, \ldots, d, \tag{22}$$

where $k = A+1, A+2, \ldots, K$. Then, the decoding matrix $\overleftarrow{\mathbf{U}}^{[k]}$ of the reverse direction can be obtained by combining the vectors of $\overleftarrow{\mathbf{U}}_{\star s}^{[k]}$. Thus, we can set the precoding matrices of the $(A+1)$th SBS to the Kth SBS as $\mathbf{V}^{[k]} = \overleftarrow{\mathbf{U}}^{[k]}$. The iterations between the forward and reverse directions continue until the algorithm converges, which is similar to the MinIL algorithm in [31].

Using the above process, the precoding matrices $\mathbf{V}$, the decoding vectors $\mathbf{u}$ and matrices $\mathbf{U}$ can be obtained. Based on these solutions, we can calculate the precoding matrices of jamming signal by zero-forcing. The jamming covariance matrices in the reverse direction can be expressed as

$$\begin{aligned}\overleftarrow{\mathbf{Q}}_{jam}^{[j]} = &\sum_{i=1}^{A} P_1\overleftarrow{\mathbf{G}}^{[ji]}\overleftarrow{\mathbf{V}}^{[i]}\overleftarrow{\mathbf{V}}^{[i]\dagger}\overleftarrow{\mathbf{G}}^{[ji]\dagger} \\ &+ \sum_{l=A+1}^{K} \frac{P_2}{d}\overleftarrow{\mathbf{G}}^{[jl]}\overleftarrow{\mathbf{V}}^{[l]}\overleftarrow{\mathbf{V}}^{[l]\dagger}\overleftarrow{\mathbf{G}}^{[jl]\dagger}, \forall j = 1, 2, \ldots, A,\end{aligned} \tag{23}$$

where $\overleftarrow{\mathbf{G}}^{[ji]} = \mathbf{G}^{[ij]\dagger}$.

Then, the jamming precoding matrix $\mathbf{\Gamma}^{[j]}$ $(j = 1, 2, \ldots, A)$ can be obtained by combining the vectors $\mathbf{\Gamma}_{\star s}^{[j]}$ expressed as

$$\mathbf{\Gamma}_{\star s}^{[j]} = \mathbf{v}_s\left(\overleftarrow{\mathbf{Q}}_{jam}^{[j]}\right), s = 1, \ldots, d_{jam}. \tag{24}$$

Thus, the distributed algorithm for the proposed scheme can be summarized as Algorithm 1. According to [31], Algorithm 1 can be implemented distributedly in two ways. (1) The algorithm can be implemented through communication and training in the forward and reverse directions iteratively until convergence, in which only local CSI needs to be estimated. (2) If the global CSI is available at each node, precoding and decoding matrices can be calculated at each node distributedly following Algorithm 1.

According to the above algorithm, all the interference and jamming signal can be eliminated perfectly at each legitimate user when the feasibility conditions can be satisfied, which can be performed at each node in a distributed way.

IV. Feasibility Conditions

In order to eliminate the interference and jamming signal perfectly at each legitimate user, the feasibility conditions

Algorithm 1 Distributed Algorithm for the Proposed Scheme

1: Start with arbitrary $M \times d$ matrices $\mathbf{V}^{[l]}$ with $\mathbf{V}^{[l]}\mathbf{V}^{[l]\dagger} = \mathbf{I}_d, \forall i = A+1, A+2, \ldots, K$.
2: **repeat**
3: In the forward direction, calculate the interference covariance matrix $\mathbf{Q}^{[k]}$ at the kth user according to (17) and (18), $k = 1, \ldots, K$.
4: Compute the decoding matrix $\mathbf{u}^{[i]}$ at the ith user and $\mathbf{U}^{[l]}$ at the lth user according to (20) and (19), respectively, $i = 1, \ldots, A$, $l = A+1, \ldots, K$.
5: Reverse the direction. $\overleftarrow{\mathbf{H}}^{[kj]} = \mathbf{H}^{[jk]\dagger}$, $\overleftarrow{\mathbf{v}}^{[i]} = \mathbf{u}^{[i]}$, and $\overleftarrow{\mathbf{V}}^{[l]} = \mathbf{U}^{[l]}$.
6: Calculate $\overleftarrow{\mathbf{Q}}^{[k]}$ according to (21), $k = A+1, \ldots, K$.
7: Compute the decoding matrix $\overleftarrow{\mathbf{U}}^{[k]}$ according to (22), $k = A+1, A+2, \ldots, K$.
8: Reverse the communication direction. $\mathbf{V}^{[k]} = \overleftarrow{\mathbf{U}}^{[k]}, k = A+1, A+2, \ldots, K$.
9: **until** convergence
10: Calculate $\overleftarrow{\mathbf{Q}}^{[j]}_{jam}$ according to (23), $j = 1, 2, \ldots, A$.
11: Compute $\mathbf{\Gamma}^{[j]}$ according to (24), $j = 1, 2, \ldots, A$.
12: Output the solutions as $\mathbf{V}^{[k]}, k = A+1, \ldots, K$, $\mathbf{u}^{[j]}, j = 1, \ldots, A$, $\mathbf{U}^{[k]}, k = A+1, \ldots, K$ and $\mathbf{\Gamma}^{[j]}, j = 1, \ldots, A$.

should be satisfied, through which the minimal number of antennas can be obtained to achieve perfect IA. In [35], Yetis *et al*. demonstrated that the feasibility conditions can be derived by comparing the number of equations and the number of variables. In this section, the feasibility conditions for the proposed UAV assisted hyper-dense network are derived first without considering jamming signal. Then, the feasibility conditions for the jamming signal are also derived.

A. Feasibility Conditions of the UAV Assisted Network

According to Bezout's theorem, a general polynomial system can be solved if and only if the number of equations does not exceed that of variables. Thus, an IA network can be classified as feasible or infeasible by comparing the number of equations with that of variables in [35]. Correspondingly, the proper conditions for the proposed scheme can be derived in Theorem 1 based on Lemma 1 and Lemma 2.

Lemma 1: The total number of equations in (4)-(7) can be calculated as

$$\begin{aligned}\mathcal{N}_\varepsilon = &A(A-1) + A(K-A)d + (K-A)Ad \\ &+ (K-A)(K-A-1)d^2.\end{aligned} \tag{25}$$

Proof: First, the number of equations in (4) can be derived as

$$\mathcal{N}_{\varepsilon 1} = A(A-1). \tag{26}$$

Then, we can obtain the number of equations in (5) as

$$\mathcal{N}_{\varepsilon 2} = A(K-A)d. \tag{27}$$

We can also know that the number of equations in (6) can be denoted as

$$\mathcal{N}_{\varepsilon 3} = (K-A)Ad. \tag{28}$$

Besides, the number of equations in (7) can be expressed as

$$\mathcal{N}_{\varepsilon 4} = (K-A)(K-A-1)d^2. \tag{29}$$

Thus, the total number of equations in (4)-(7) can be calculated as

$$\begin{aligned}\mathcal{N}_\varepsilon =&\mathcal{N}_{\varepsilon 1} + \mathcal{N}_{\varepsilon 2} + \mathcal{N}_{\varepsilon 3} + \mathcal{N}_{\varepsilon 4} \\ =&A(A-1) + A(K-A)d \\ &+ (K-A)Ad + (K-A)(K-A-1)d^2.\end{aligned} \tag{30}$$

■

Lemma 2: The total number of variables in (4)-(7) can be calculated as

$$\mathcal{N}_v = A(N-1)+(K-A)(N-d)d+(K-A)(M-d)d. \tag{31}$$

Proof: The total number of variables in the decoding vectors $\mathbf{u}^{[i]}$, $i = 1, 2, \ldots, A$, can be denoted as

$$\mathcal{N}_{v1} = A(N-1). \tag{32}$$

The total number of variables in the decoding matrices $\mathbf{U}^{[l]}$, $l = A+1, A+2, \ldots, K$, can be expressed as

$$\mathcal{N}_{v2} = (K-A)(N-d)d. \tag{33}$$

In addition, the number of variables in the precoding matrices $\mathbf{V}^{[k]}$, $k = A+1, A+2, \ldots, K$, can be calculated as

$$\mathcal{N}_{v3} = (K-A)(M-d)d. \tag{34}$$

Thus, the total number of variables in (4)-(7) can be caculated as

$$\begin{aligned}\mathcal{N}_v =&\mathcal{N}_{v1} + \mathcal{N}_{v2} + \mathcal{N}_{v3} \\ =&A(N-1)+(K-A)(N-d)d+(K-A)(M-d)d.\end{aligned} \tag{35}$$

■

Theorem 1: The proper conditions of the proposed UAV assisted hyper-dense network can be expressed as (36) (on the next page).

Proof: According to [35], the proposed scheme is feasible if and only if $\mathcal{N}_\varepsilon \leq \mathcal{N}_v$. Thus, according to Lemma 1 and Lemma 2, the proposed scheme is proper if and only if (37) is satisfied (on the next page), which can be simplified as the first inequality in (36).

Besides, each of the $(A+1)$th user to the Kth user should recover d streams transmitted by its corresponding SBS. According to the DoF requirement of MIMO network, the values of M and N should satisfy $M \geq d$ and $N \geq d$.

Furthermore, we can notice that the solutions to (4) and (6) only depend on the decoding matrices. Thus, the feasible value of N can be obtained by comparing the total number of variables in (4) and (6) with that of equations in (4) and (6). According to Lemma 1, the total number of the equations in (4) and (6) can be given by

$$\mathcal{N}_{\varepsilon 1} + \mathcal{N}_{\varepsilon 3} = A(A-1) + (K-A)Ad. \tag{38}$$

According to Lemma 2, the total number of the variables in (4) and (6) can be expressed as

$$\mathcal{N}_{v1} + \mathcal{N}_{v2} = A(N-1) + (K-A)(N-d)d. \tag{39}$$

In order to make (4) and (6) solvable, the total number of their

$$\begin{aligned} AN+(K-A)(M+N)d &\geq A^2+A^2d^2-2A^2d+K^2d^2-2KAd^2+2AKd+Kd^2-Ad^2, \\ N &\geq d+A-\frac{Ad}{(K-A)d+A}, \\ M &\geq d. \end{aligned} \tag{36}$$

$$A(N-1)+(K-A)(N-d)d+(K-A)(M-d)d \geq A(A-1)+A(K-A)d+(K-A)Ad+(K-A)(K-A-1)d^2. \tag{37}$$

variables should be no less than that of their equations as

$$\begin{aligned} \mathcal{N}_{v1}+\mathcal{N}_{v2} &\geq \mathcal{N}_{\varepsilon 1}+\mathcal{N}_{\varepsilon 3}, \\ A(N-1)+(K-A)(N-d)d &\geq A(A-1)+(K-A)Ad, \end{aligned} \tag{40}$$

which can be simplified as

$$N \geq d+A-\frac{Ad}{(K-A)d+A}. \tag{41}$$

Therefore, from the above analysis, the proper conditions of the proposed scheme can be derived as (36). ■

According to the conclusions in [35], the proper condition is not always equivalent to the feasibility condition in IA. Nevertheless, the proper system is feasible in most of the cases with few counter-examples. In addition, the proposed Algorithm 1 can also be adopted as a theoretical tool for examining the feasibility of the proposed scheme off-line.

B. Feasibility Conditions of the Jamming Signal

In the proposed scheme, the jamming signal should be generated by the idle SBSs to disrupt the potential eavesdropping without affecting the legitimate transmission. Thus, the jamming signal should be constrained into the same subspace of the interference at each user, i.e., conditions (15) and (16) should be satisfied by designing the precoding matrices of jamming properly.

Lemma 3: The total number of equations in (15) and (16) can be calculated as

$$\mathcal{N}_{\varepsilon}^{jam}=A^2d_{jam}+A(K-A)dd_{jam}. \tag{42}$$

Proof: The number of equations in (15) can be given as

$$\mathcal{N}_{\varepsilon 5}=A^2d_{jam}. \tag{43}$$

In addition, the number of equations in (16) can be given as

$$\mathcal{N}_{\varepsilon 6}=A(K-A)dd_{jam}. \tag{44}$$

Thus, the total number of equations in (15) and (16) can be given as $\mathcal{N}_{\varepsilon}^{jam}=\mathcal{N}_{\varepsilon 5}+\mathcal{N}_{\varepsilon 6}=A^2d_{jam}+A(K-A)dd_{jam}$. ■

Lemma 4: The total number of variables in (15) and (16) can be calculated as

$$\mathcal{N}_{v}^{jam}=Ad_{jam}(M_{jam}-d_{jam}). \tag{45}$$

Proof: Due to the fact that the decoding matrices in (15) and (16) have been determined by the proposed scheme, the effective variables in (15) and (16) only exist in the precoding matrices $\mathbf{\Gamma}^{[j]}$ for jamming signal. Thus, the total number of variables in (15) and (16) can be derived as $\mathcal{N}_{v}^{jam}=\mathcal{N}_{v4}=Ad_{jam}(M_{jam}-d_{jam})$. ■

Theorem 2: The feasibility condition of the jamming signal for the proposed scheme can be expressed as (46).

$$M_{jam} \geq A+(K-A)d+d_{jam}. \tag{46}$$

Proof: It is known that $\mathcal{N}_{v}^{jam} \geq \mathcal{N}_{\varepsilon}^{jam}$ should be satisfied to make (15) and (16) solvable. Thus according to Lemma 3 and Lemma 4, we have $Ad_{jam}(M_{jam}-d_{jam}) \geq A^2d_{jam}+A(K-A)dd_{jam}$, which can be simplified as (46). ■

Remark 2: The minimal number of antennas equipped at SBSs and users to perfectly eliminate the interference between users can be determined by the feasibility conditions in Theorem 1. Then, based on the proposed scheme, the minimal number of antennas to generate jamming signal, which can be zero-forced at the legitimate users, can be determined by the feasibility condition in Theorem 2.

V. Performance Analysis of the Eavesdropper

In the proposed scheme, the 1st to the Ath SBSs are replaced by UAVs to provide video streaming service to mobile users, and thus, these A SBSs can be exploited to generate jamming signal to guarantee the security of the legitimate transmission. Thus, in this section, the eavesdropping performance is analyzed with and without jamming signal, respectively, to show the effectiveness of the proposed jamming design in secure transmission[3].

A. Eavesdropping Performance without Jamming Signal

As mentioned in Section, an eavesdropper with N_e antennas exists in the UAV assisted hyper-dense network. We assume that the CSI between the legitimate transmitters and the eavesdropper can be obtained by the eavesdropper. However, the CSI between the legitimate transmitters and mobile users are unavailable at the eavesdropper, and thus, the number of data streams for each transmitter is difficult to know at the eavesdropper.

First, we consider the case when the eavesdropper attempts to eavesdrop the information for the ith legitimate user served by the UAV, $i=1,2,\ldots,A$. When decoding is performed at

[3]In the proposed scheme, the jamming signal can be eliminated together with the interference between legitimate users, which will not affect the legitimate transmission rate when feasibility conditions can be met. Thus, we can just examine the eavesdropping rate to verify the effectiveness of jamming signal on the secrecy rate.

the eavesdropper, the recovered signal without jamming signal can be expressed as

$$y_{e-1}^{[i]} = \mathbf{u}_e^{[i]\dagger}\mathbf{h}_e^{[i]}x^{[i]} + \sum_{a=1,a\neq i}^{A}\mathbf{u}_e^{[i]\dagger}\mathbf{h}_e^{[a]}x^{[a]} + \sum_{k=A+1}^{K}\mathbf{u}_e^{[i]\dagger}\mathbf{H}_e^{[k]}\mathbf{V}^{[k]}\mathbf{x}^{[k]} + \mathbf{u}_e^{[i]\dagger}\mathbf{z}_e, \tag{47}$$

where $\mathbf{u}_e^{[i]}$ is $N_e \times 1$ decoding vector for the eavesdropper to obtain the information of the ith user.

In order to eliminate the interference from other users effectively, the following conditions should be satisfied.

$$\mathbf{u}_e^{[i]\dagger}\mathbf{h}_e^{[a]} = 0, \forall a = 1, 2, \ldots, A, a \neq i, \tag{48}$$

$$\mathbf{u}_e^{[i]\dagger}\mathbf{H}_e^{[k]}\mathbf{V}^{[k]} = \mathbf{0}, \forall k = A+1, A+2, \ldots, K. \tag{49}$$

To make (48) and (49) solvable, enough antennas should be equipped at the eavesdropper. The minimal required number of antennas by the eavesdropper is derived in Proposition 1.

Proposition 1: For the eavesdropper in the proposed scheme without jamming signal, at least $(K-A)d + A$ antennas are needed to eavesdrop the ith user served by the UAV with inter-user interference perfectly eliminated.

Proof: The total number of equations in (48) and (49) can be expressed as

$$\mathcal{N}_{\varepsilon-1}^{e} = (A-1) + (K-A)d. \tag{50}$$

Since the precoding matrices in (49) are determined by the proposed scheme, the effective variables in (48) and (49) only exist in the decoding vector $\mathbf{u}_e^{[i]}$ of the eavesdropper, which can be expressed as

$$\mathcal{N}_{v-1}^{e} = N_e - 1. \tag{51}$$

Therefore, (48) and (49) can be solved only when $\mathcal{N}_{v-1}^{e} \geq \mathcal{N}_{\varepsilon-1}^{e} \Rightarrow N_e \geq (K-A)d + A$. ■

Based on Proposition 1, we can know that the eavesdropping rate of the ith user, $i = 1, 2, \ldots, A$, can be expressed as

$$R_{e-1}^{[i]} = \log_2\left(1+\frac{P_1\mathbf{u}_e^{[i]\dagger}\mathbf{h}_e^{[i]}\mathbf{h}_e^{[i]\dagger}\mathbf{u}_e^{[i]}}{\sigma^2}\right). \tag{52}$$

On the other hand, we consider the case when the eavesdropper wants to eavesdrop the lth legitimate user served by the SBS, $l = A+1, A+2, \ldots, K$. When decoding is performed, the recovered signal at the eavesdropper can be written as

$$y_{e-2}^{[l]} = \sum_{s=1}^{d}\mathbf{u}_e^{[l]\dagger}\mathbf{H}_e^{[l]}\mathbf{V}_{\star s}^{[l]}x_s^{[l]} + \sum_{a=1}^{A}\mathbf{u}_e^{[l]\dagger}\mathbf{h}_e^{[a]}x^{[a]} + \sum_{\substack{k=A+1\\k\neq l}}^{K}\mathbf{u}_e^{[l]\dagger}\mathbf{H}_e^{[k]}\mathbf{V}^{[k]}\mathbf{x}^{[k]} + \mathbf{u}_e^{[l]\dagger}\mathbf{z}_e, \tag{53}$$

where $x_s^{[l]}$ is the sth data stream for the lth user. To eliminate the interference from other users, the following conditions should be satisfied:

$$\mathbf{u}_e^{[l]\dagger}\mathbf{h}_e^{[a]} = 0, \forall a = 1, 2, \ldots, A, \tag{54}$$

$$\mathbf{u}_e^{[l]\dagger}\mathbf{H}_e^{[k]}\mathbf{V}^{[k]} = 0, \forall k = A+1, A+2, \ldots, K, l \neq k. \tag{55}$$

Similar to Proposition 1, we can conclude that if we want to eliminate the inter-user interference from other legitimate user when eavesdropping a certain SBS served user, the following condition should be satisfied.

$$N_e \geq (K-A-1)d + A + 1. \tag{56}$$

Nevertheless, the interference of other data streams of this user cannot be eliminated. Therefore, the eavesdropping rate of the lth user, $l = A+1, A+2, \ldots K$, can be calculated as

$$R_{e-2}^{[l]} = \sum_{s=1}^{d}\log_2\left(1+\frac{P_2\mathbf{u}_e^{[l]\dagger}\mathbf{H}^{[el]}\mathbf{V}_{\star s}^{[l]}\mathbf{V}_{\star s}^{[l]\dagger}\mathbf{H}^{[el]\dagger}\mathbf{u}_e^{[l]}}{d\sigma^2 + P_2\sum\limits_{i=1,i\neq s}^{d}\mathbf{u}_e^{[l]\dagger}\mathbf{H}^{[el]}\mathbf{V}_{\star i}^{[l]}\mathbf{V}_{\star i}^{[l]\dagger}\mathbf{H}^{[el]\dagger}\mathbf{u}_e^{[l]}}\right). \tag{57}$$

B. Eavesdropping Performance with Jamming Signal

When the jamming signal is generated by the idle SBSs, the potential eavesdropping will be disrupted. According to Proposition 1, when the eavesdropper is equipped with $(K-A)d+A$ antennas and attempts to eavesdrop the ith user served by the UAV, $i = 1, 2, \ldots, A$, we can know that the interference from other legitimate users can be eliminated. The recovered signal at the eavesdropper can be expressed as

$$y_{e-1}^{*[i]} = \mathbf{u}_e^{[i]\dagger}\mathbf{h}_e^{[i]}x^{[i]} + \sum_{j=1}^{A}\mathbf{u}_e^{[i]\dagger}\mathbf{G}_e^{[j]}\mathbf{\Gamma}^{[j]}\mathbf{x}_{jam}^{[j]} + \mathbf{u}_e^{[i]\dagger}\mathbf{z}_e, \tag{58}$$

and the eavesdropping rate can be rewritten as

$$R_{e-1}^{*[i]} = \log_2\left(1+\frac{P_1\mathbf{u}_e^{[i]\dagger}\mathbf{h}_e^{[i]}\mathbf{h}_e^{[i]\dagger}\mathbf{u}_e^{[i]}}{\sigma^2 + \frac{P_{jam}}{d_{jam}}\sum_{j=1}^{A}\mathbf{u}_e^{[i]\dagger}\mathbf{G}_e^{[j]}\mathbf{\Gamma}^{[j]}\mathbf{\Gamma}^{[j]\dagger}\mathbf{G}_e^{[j]\dagger}\mathbf{u}_e^{[i]}}\right). \tag{59}$$

Similarly, when the eavesdropper is equipped with $(K-A-1)d + A + 1$ antennas and attempts to eavesdrop the lth user served by the SBS, $l = A+1, A+2, \ldots, K$, the interference from other user can be eliminated. The recovered signal at the eavesdropper can be expressed as

$$y_{e-2}^{*[l]} = \sum_{s=1}^{d}\mathbf{u}_e^{[l]\dagger}\mathbf{H}_e^{[l]}\mathbf{V}_{\star s}^{[l]}x_s^{[l]} + \sum_{j=1}^{A}\mathbf{u}_e^{[l]\dagger}\mathbf{G}_e^{[j]}\mathbf{\Gamma}^{[j]}\mathbf{x}_{jam}^{[j]} + \mathbf{u}_e^{[l]\dagger}\mathbf{z}_e, \tag{60}$$

and the eavesdropping rate can be rewritten as (61) (on the next page).

Remark 3: According to (52), (57), (59) and (61), we can conclude that $R_{e-2}^{[l]} > R_{e-2}^{*[l]}$ and $R_{e-1}^{[i]} > R_{e-1}^{*[i]}$ for the same number of eavesdropping antennas, due to jamming. However, the transmission rate of the legitimate users will not be changed by the jamming signal. Thus, the secrecy rate of the legitimate users will be increased through introducing the jamming signal into the network. In addition, when the transmit power of the jamming signal P_{jam} becomes larger, the secrecy rate will increase accordingly.

Next, the case when more antennas are equipped at the eavesdropper to eliminate the jamming signal is analyzed. According to (58) and (60), in order to eliminate the jamming

$$R_{e-2}^{*[l]} = \sum_{s=1}^{d} \log_2 \left(1 + \frac{P_2 \mathbf{u}_e^{[l]\dagger} \mathbf{H}_e^{[l]} \mathbf{V}_{\star s}^{[l]} \mathbf{V}_{\star s}^{[l]\dagger} \mathbf{H}_e^{[l]\dagger} \mathbf{u}_e^{[l]}}{d\sigma^2 + P_2 \sum_{i=1, i\neq s}^{d} \mathbf{u}_e^{[l]\dagger} \mathbf{H}_e^{[l]} \mathbf{V}_{\star i}^{[l]} \mathbf{V}_{\star i}^{[l]\dagger} \mathbf{H}_e^{[l]\dagger} \mathbf{u}_e^{[l]} + d\frac{P_{jam}}{d_{jam}} \sum_{j=1}^{A} \mathbf{u}_e^{[l]\dagger} \mathbf{G}_e^{[j]} \mathbf{\Gamma}^{[j]} \mathbf{\Gamma}^{[j]\dagger} \mathbf{G}_e^{[j]\dagger} \mathbf{u}_e^{[l]}} \right). \quad (61)$$

signal, the following condition should be satisfied along with (48) and (49) or (54) and (55):

$$\mathbf{u}_e^{[k]\dagger} \mathbf{G}_e^{[j]} \mathbf{\Gamma}^{[j]} = \mathbf{0}. \quad (62)$$

When the eavesdropper wants to eavesdrop the information of the ith user served by UAV, $i = 1, 2, \ldots, A$, (48), (49) and (62) should be all satisfied, and the minimal required number of antennas of the eavesdropper is derived in Proposition 2.

Proposition 2: For the eavesdropper, at least $(K - A)d + A + Ad_{jam}$ antennas should be equipped to eavesdrop the ith user served by UAV without interference from other users and jamming signal, $i = 1, 2, \ldots, A$.

Proof: The number of equations in (62) is equal to Ad_{jam}. Thus, according to (50), the total number of equations in (48), (49) and (62) can be expressed as

$$\mathcal{N}_{\varepsilon-2}^{e} = (A - 1) + (K - A)d + Ad_{aj}. \quad (63)$$

The total number of variables in (48), (49) and (62) can still be expressed as (51). Thus, (48), (49) and (62) can be solved only when $\mathcal{N}_{v-2}^{e} \geq \mathcal{N}_{\varepsilon-2}^{e} \Rightarrow N_e \geq (K-A)d+A+Ad_{jam}$. ■

Similar to Proposition 2, when the eavesdropper wants to eavesdrop the information of the lth user served by the SBS, $l = A + 1, A + 2, \ldots, K$, at least

$$N_e = (K - A - 1)d + A + 1 + Ad_{jam} \quad (64)$$

antennas should be equipped to eliminate the interference from other legitimate users and jamming signal perfectly.

Remark 4: According to the above analysis, we can conclude that Ad_{jam} more antennas should be equipped at the eavesdropper to successfully eavesdrop the kth user when jamming signal is generated by the idle SBSs. In other words, the eavesdropper should make more effort to eavesdrop the kth user when jamming signal is generated.

VI. Numerical Results and Discussion

In this section, the performance of the proposed UAV assisted hyper-dense small-cell network is presented and verified through extensive simulations. We assume that the transmit power of UAVs and SBSs are equal, i.e., $P_1 = P_2 = P_{jam} = 1$.

The sum rate of the small-cell network with different numbers of M and N is shown in Fig. 3 without jamming signal, where $K = 5$, $A = 2$, and $d = 1$. From the results, we can see that the sum rate will increase linearly with SNR only when the feasibility conditions in Theorem 1 can be satisfied, i.e., $5N + 3M \geq 28$ and $N \geq 3$, and all the interference can be eliminated. When $5N + 3M < 28$, we can see that the sum rate of the network is much lower than that when it is feasible, due to the residual interference. In addition, based on the feasibility numbers of M and N, the sum rate of the network with the jamming signal is also compared in Fig. 3 for

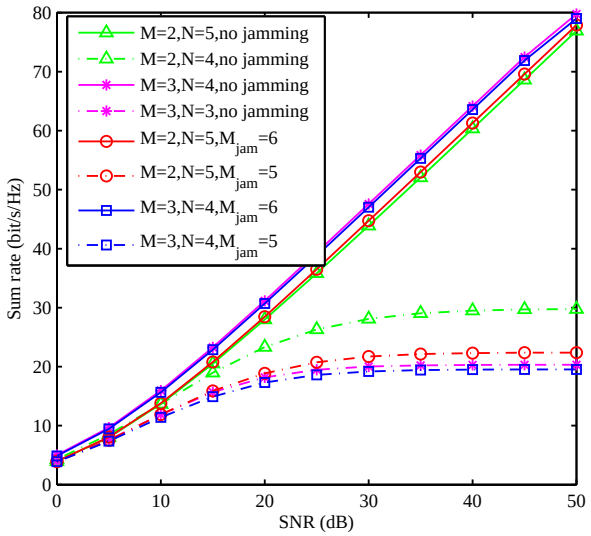

Fig. 3. Sum rate comparison of the small-cell network with and without jamming signal, with different number of antennas equipped at each SBS, each mobile user and each jammer ($K = 5$, $A = 2$, and $d = 1$).

different numbers of antennas equipped at the jammers, M_{jam}, when the feasibility conditions in Theorem 1 are satisfied. $K = 5$, $A = 2$, $d = 1$, and $d_{jam} = 1$. From the results, we can see that the interference can be perfectly eliminated and the sum rate of the network increases linearly with SNR, only when the feasibility condition of the jamming in Theorem 2 can be satisfied, i.e., $M_{jam} \geq 6$. In addition, we can see that the the feasible value of M_{jam} only depends on A, K, d and d_{jam}, instead of M and N.

To further verify the feasibility conditions in Theorem 1, the interference leakage at each mobile user with different values of M and N is compared in Fig. 4, without jamming, when $K = 5$, $A = 2$, $d = 2$, and SNR=25dB. From the results, we can note that the interference leakage can be eliminated perfectly only when the feasibility conditions in Theorem 1 can be satisfied, i.e., $3M + 4N \geq 38$ and $N \geq 4$. We can also see that, when M becomes smaller, larger N is needed to make it feasible.

Similarly, to verify the feasibility condition in Theorem 2, we compare the interference leakage at each mobile user with different values of d, d_{jam}, M and N in Fig. 5, with jamming signal generated, when $K = 5$, $A = 2$ and SNR=25dB. From the results, we can see that only when the feasibility condition $M_{jam} \geq A+(K-A)d+d_{jam}$ in Theorem 2 can be satisfied, the interference can be eliminated perfectly. In addition, we can find that the feasible value of M_{jam} is only related to the values of d, d_{jam}, K and A, and it will not be affected by the values of M and N when the feasibility conditions in Theorem 1 have already been satisfied.

When the eavesdropper intends to eavesdrop the legitimate

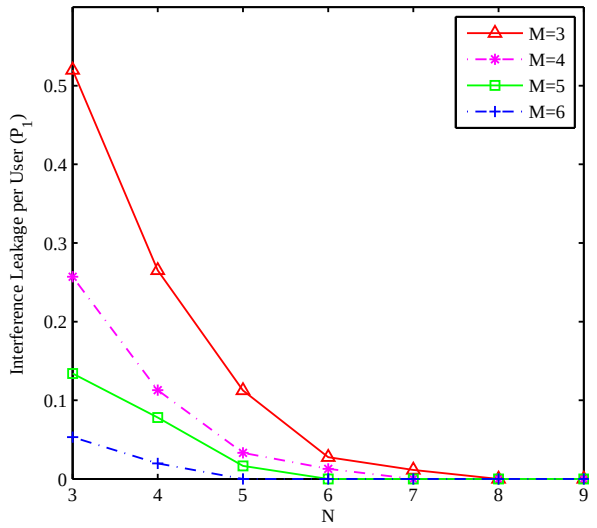

Fig. 4. Comparison of interference leakage at each mobile user with different values of M and N. ($K = 5$, $A = 2$, $d = 2$ and SNR=25dB).

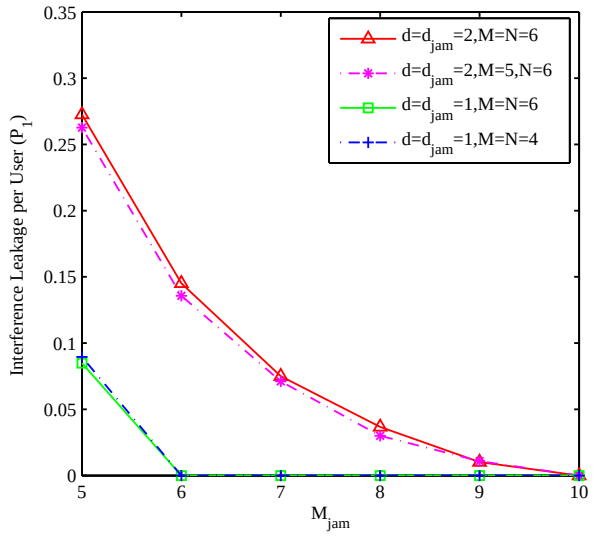

Fig. 5. Comparison of interference leakage at each mobile user with different values of M_{jam}. ($K = 5$, $A = 2$ and SNR=25dB).

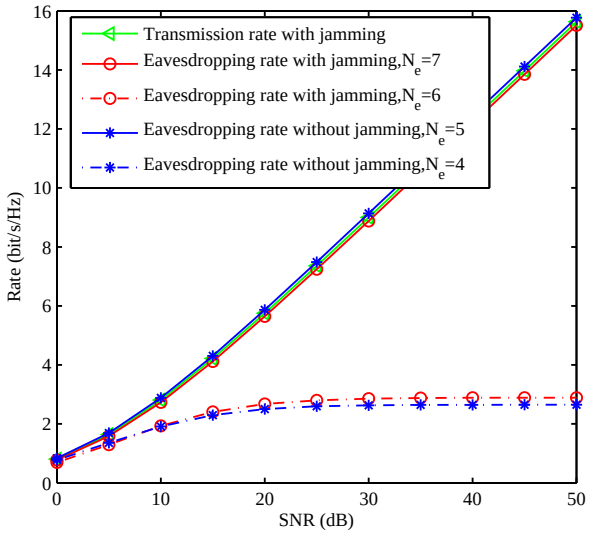

Fig. 6. Comparison of the transmission and eavesdropping rate of a certain UAV served user in the small-cell network with different numbers of N_e. ($K = 5$, $A = 2$, $M = N = 4$, $d = 1$, and $d_{jam} = 1$).

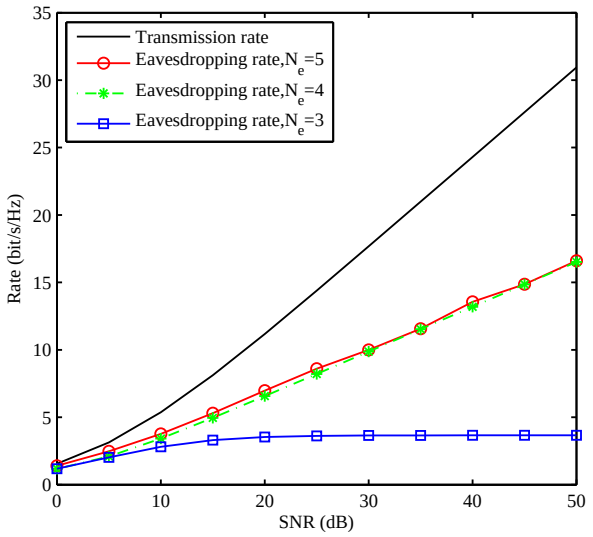

Fig. 7. Comparison of the transmission and eavesdropping rate of a certain SBS served user in the small-cell network without jamming signal, with different number of N_e. ($K = 3$, $A = 1$, $M = N = 4$, and $d = 2$).

transmission of a certain UAV, the transmission and eavesdropping rate of a certain UAV served user is compared in Fig. 6 with different number of N_e, with or without jamming signal. We also assume that the legitimate network is feasible with $K = 5$, $A = 2$, $d = 1$, $M = N = 4$, $d_{jam} = 1$ and $M_{jam} = 6$ according to Theorem 1. From the results, we can note that when no jamming is generated, at least $N_e = 5$ antennas are needed to perfectly eavesdrop a certain UAV served user, which is consistent with the conclusion in Proposition 1. On the other hand, we can also see that when jamming signal is generated by the idle SBSs, at least $N_e = 7$ antennas should be equipped at the eavesdropper to eavesdrop a certain UAV served user, which is consistent with the conclusion in Proposition 2. Therefore, we can conclude that additional $Ad_{jam} = 2$ antennas should be equipped at the eavesdropper to successfully eavesdrop a UAV served user when jamming signal is generated by the idle SBSs, compared to the case without jamming signal. In other words, the jamming signal can make the legitimate network much securer.

In Fig. 7, the transmission and eavesdropping rate of a certain SBS served user is compared without jamming signal, when an eavesdropper intends to eavesdrop its transmission. We set $K = 3$, $A = 1$, $d = 2$ and $M = N = 4$ to make the small-cell network feasible, according to Theorem 1. From the results, we can observe that the eavesdropping rate is very low when $N_e < 4$, due to the fact the interference cannot be perfectly eliminated at the eavesdropper, which will affect its eavesdropping performance. When $N_e \geq 4$, the eavesdropping rate increases linearly with SNR, which has been greatly improved, according to the conclusion in (56). However, the

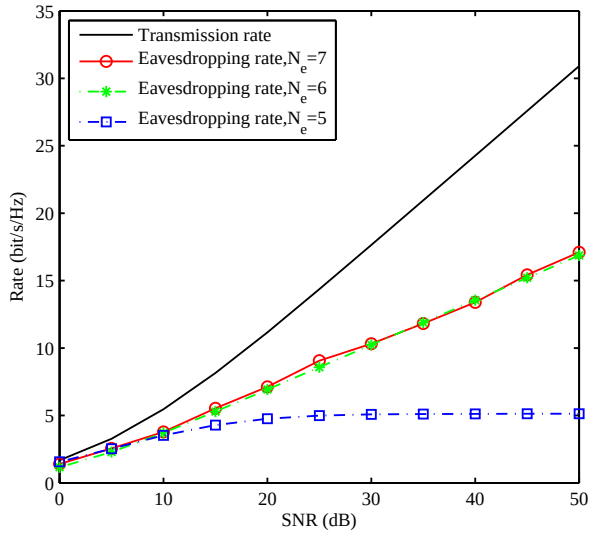

Fig. 8. Comparison of the transmission and eavesdropping rate of a certain SBS served user in the small-cell network with jamming signal, with different numbers of N_e. ($K = 3$, $A = 1$, $M = N = 4$, $M_{jam} = 7$, $d = 2$, and $d_{jam} = 2$).

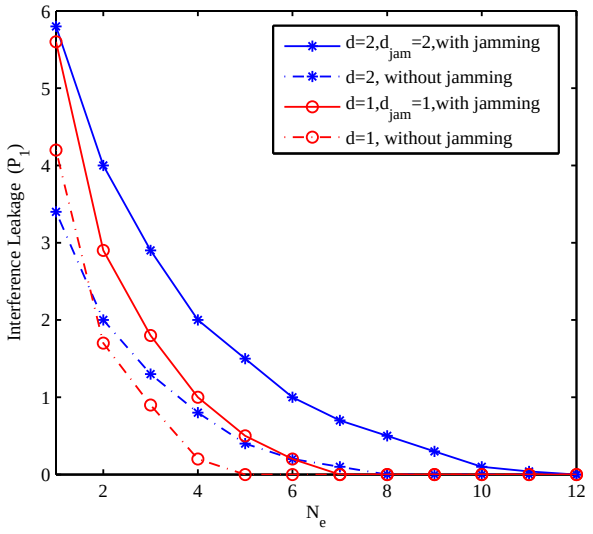

Fig. 9. Comparison of interference leakage at the eavesdropper with different number of N_e when the eavesdropper tries to eavesdrop a certain UAV served user ($K = 5$, $A = 2$, $M = N = 6$, $M_{jam} = 10$ and SNR=25dB).

achieved eavesdropping rate is also lower than the transmission rate, due to the fact the the interference between data streams of the SBS served user cannot be eliminated by the eavesdropper. Then, similar results are provided in Fig. 8, in which the jamming signal is considered. We set $K = 3$, $A = 1$, $d = 2$, $M_{jam} = 7$, $d_{jam} = 2$ and $M = N = 4$ to make the small-cell network feasible, according to Theorem 1 and Theorem 2. Comparing the results in Fig. 7 and Fig. 8, we can conclude that $Ad_{jam} = 2$ more antennas should be equipped at the eavesdropper to eavesdrop a certain SBS served user with jamming signal, compared to that without jamming signal, according to the conclusion in (56) and (64). Thus, the proposed scheme with jamming signal can make the network much securer.

The interference leakage at the eavesdropper with different number of N_e when the eavesdropper tries to eavesdrop a certain UAV served user or a SBS served user, is compared in Fig. 9 and Fig. 10, respectively. $K = 5$, $A = 2$, $M = N = 6$ and $M_{jam} = 10$ are set to make the legitimate network feasible, according to Theorem 1 and Theorem 2. SNR=25dB. From the results in Fig. 9, we can see that the interference leakage can be perfectly eliminated at the eavesdropper aiming at a certain UAV served user, only when enough antennas are equipped at the eavesdropper to satisfy the conditions in Proposition 1 or Proposition 2. Especially, larger d, larger d_{jam} can make the user more difficult to eavesdrop. From the results in Fig. 10, we can note that the interference between users can be perfectly eliminated at the eavesdropper aiming at a certain SBS served user, only when enough antennas are equipped at the eavesdropper to satisfy the conclusions in (56) or (64). In addition, when $d = 2$, there exists some residual interference, due to the fact that the interference between data streams of the target user cannot be eliminated perfectly.

Finally, the transmission and eavesdropping rate of a targeted UAV served user is compared in Fig. 11, when the

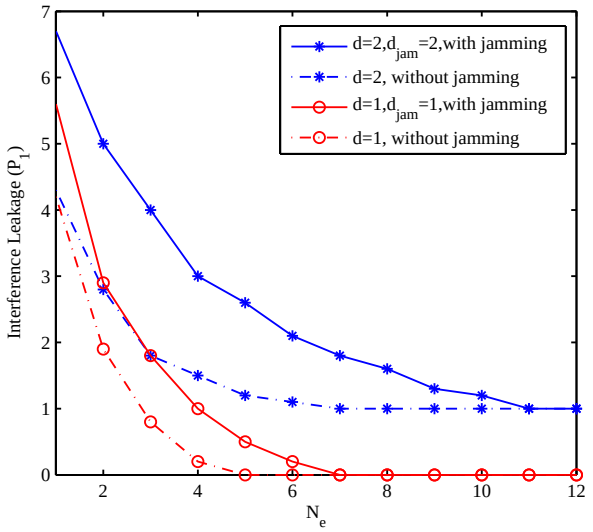

Fig. 10. Comparison of interference leakage at the eavesdropper with different number of N_e when the eavesdropper tries to eavesdrop a certain SBS served user ($K = 5$, $A = 2$, $M = N = 6$, $M_{jam} = 10$ and SNR=25dB).

transmit power of the jamming signal P_{jam} becomes larger. $K = 5$, $A = 2$, $M = N = 6$, $M_{jam} = 10$ and $d = d_{jam} = 2$ are set to make the scheme feasible according to Theorem 1 and Theorem 2. SNR=25dB. From the results, we can see that when $N_e < 12$, the transmission of the user cannot be perfectly eavesdropper, which is consistent with the conclusion of Proposition 2. In addition, we can find that the eavesdropping rate will decrease with higher P_{jam} or smaller N_e. Thus, we can increase P_{jam}, d or d_{jam} to guarantee the secure transmission of the legitimate network.

VII. Conclusions and Future Work

In this paper, a caching UAV assisted secure transmission scheme has been proposed in hyper-dense small-cell networks

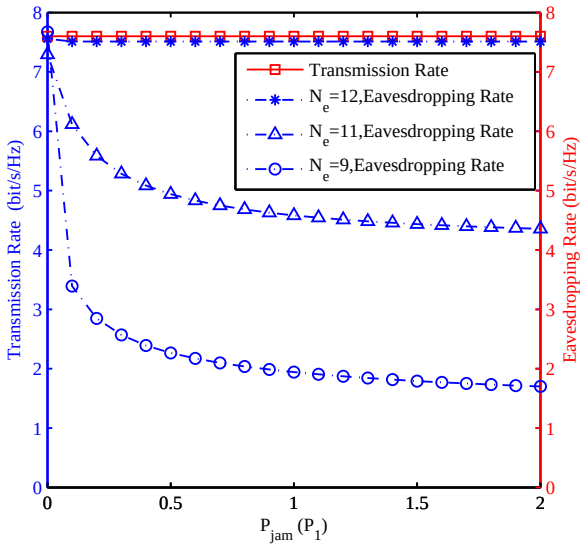

Fig. 11. Comparison of a certain UAV served user's transmission and eavesdropping rate with different number of N_e, when the transmit power of the jamming signal becomes larger ($K = 5$, $A = 2$, $M = N = 6$, $M_{jam} = 10$, $d = d_{jam} = 2$ and SNR=25dB).

based on IA. In the scheme, UAVs are utilized to provide data traffic to mobile users cooperatively with SBSs to relieve the transmission pressure of SBSs, due to the low cost and high mobility. Cache is equipped at each UAV to store popular files in advance, which can be delivered to the mobile users directly when needed at off-peak time. A single antenna is equipped at each UAV to facilitate its transmission, and the idea of IA is exploited to perform interference management in the network through designing the precoding matrices of SBS cooperatively. We derived the feasibility conditions of the proposed scheme. In addition, we proposed to use the idle SBSs replaced by UAVs to generate jamming signal to disrupt the potential eavesdropping, which would not affect the transmission of the legitimate network. Plenty of simulation results have been presented to show the effectiveness of the proposed scheme. In our future work, we will focus on the optimal wireless coverage of UAVs for the small-cell network.

ACKNOWLEDGMENT

We thank the editor and reviewers for their detailed reviews and constructive comments, which have greatly improved the quality of this paper.

REFERENCES

[1] N. Wang, E. Hossain, and V. K. Bhargava, "Backhauling 5G small cells: A radio resource management perspective," *IEEE Wireless Commun.*, vol. 22, no. 5, pp. 41–49, Oct. 2015.

[2] H. Zhang, C. Jiang, J. Cheng, and V. C. M. Leung, "Cooperative interference mitigation and handover management for heterogeneous cloud small cell networks," *IEEE Wireless Commun.*, vol. 22, no. 3, pp. 92–99, Jun. 2015.

[3] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the *K*-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[4] N. Zhao, F. R. Yu, M. Jin, Q. Yan, and V. C. M. Leung, "Interference alignment and its applications: A survey, research issues, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1779–1803, 3rd Quart. 2016.

[5] A. Dong, H. Zhang, D. Yuan, and X. Zhou, "Interference alignment transceiver design by minimizing the maximum mean square error for MIMO interfering broadcast channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6024–6037, Aug. 2016.

[6] F. C. Kavasoglu, Y. Huang, and B. D. Rao, "Semi-blind interference alignment techniques for small cell networks," *IEEE Trans. Signal Proc.*, vol. 62, no. 23, pp. 6335–6348, Dec. 2014.

[7] N. Zhao, X. Liu, F. R. Yu, M. Li, and V. C. M. Leung, "Communications, caching, and computing oriented small-cell networks with interference alignment," *IEEE Commun. Mag.*, vol. 54, no. 9, pp. 29–35, Sept. 2016.

[8] F. Cheng, Y. Yu, Z. Zhao, N. Zhao, Y. Chen, and H. Lin, "Power allocation for cache-aided small-cell networks with limited backhaul," *IEEE Access*, vol. 5, pp. 1272–1283, Jan. 2017.

[9] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[10] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[11] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[12] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, Jan. 2016.

[13] H. M. Wang, T. X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[14] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forens. Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

[15] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May. 2016.

[16] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surv. Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart. 2016.

[17] S. Koulali, E. Sabir, T. Taleb, and M. Azizi, "A green strategic activity scheduling for UAV networks: A sub-modular game perspective," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 58–64, May. 2016.

[18] V. Sharma, M. Bennis, and R. Kumar, "UAV-assisted heterogeneous networks for capacity enhancement," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1207–1210, Jun. 2016.

[19] J. Lyu, Y. Zeng, R. Zhang, and T. J. Lim, "Placement optimization of UAV-mounted mobile base stations," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 604–607, Mar. 2017.

[20] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput maximization for UAV-enabled mobile relaying systems," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, Dec. 2016.

[21] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3747–3760, Jun. 2017.

[22] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Optimal transport theory for cell association in UAV-enabled cellular networks," *IEEE Commun. Lett.*, to appear.

[23] M. Chen, M. Mozaffari, W. Saad, C. Yin, M. Debbah, and C. S. Hong, "Caching in the sky: Proactive deployment of cache-enabled unmanned aerial vehicles for optimized quality-of-experience," *IEEE J. Sel. Areas. Commun.*, vol. 35, no. 5, pp. 1046–1061, May 2017.

[24] H. Liu, Z. Chen, X. Tian, X. Wang, and M. Tao, "On content-centric wireless delivery networks," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 118–125, Dec 2014.

[25] E. Bastug, M. Bennis, and M. Debbah, "Living on the edge: The role of proactive caching in 5G wireless networks," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 82–89, Aug. 2014.

[26] Z. Zhao, M. Peng, Z. Ding, W. Wang, , and H. V. Poor, "Cluster content caching: An energy-efficient approach to improve quality of service in cloud radio access networks," *IEEE J. Sel. Areas. Commun.*, vol. 34, no. 5, pp. 1207–1221, May. 2016.

[27] C. Yang, Y. Yao, Z. Chen, , and B. Xia, "Analysis on cache-enabled wireless heterogeneous networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 131–145, Jun. 2016.

[28] M. A. Maddah-Ali and U. Niesen, "Fundamental limits of caching," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2856–2867, May 2014.

[29] M. A. Maddah-Ali and U. Niesen, "Cache-aided interference channels," in *Proc. IEEE ISIT'15*, pp. 809–813, Hong Kong, China, Jun. 2015.

[30] M. Deghel, E. Bastug, M. Assaad, and M. Debbah, "On the benefits of edge caching for MIMO interference alignment," in *Proc. IEEE SPAWC'15*, pp. 655–659, Stockholm, Sweden, Jun. 2015.

[31] K. Gomadam, V. R. Cadambe, and S. A. Jafar, "A distributed numerical approach to interference alignment and applications to wireless interference networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3309–3322, Jun. 2011.

[32] T. Xu and X. G. Xia, "A diversity analysis for distributed interference alignment using the max-sinr algorithm," *IEEE Trans. Inf. Theory*.

[33] N. Zhao, F. R. Yu, and V. C. M. Leung, "Opportunistic communications in interference alignment networks with wireless power transfer," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 88–95, Feb. 2015.

[34] N. Zhao, F. R. Yu, H. Sun, A. Nallanathan, and H. Yin, "A novel interference alignment scheme based on sequential antenna switching in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5008–5021, Oct. 2013.

[35] C. Yetis, T. Gou, S. A. Jafar, and A. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Proc.*, vol. 58, no. 9, pp. 4771–4782, Sept. 2010.

[36] S. J. Kim and G. B. Giannakis, "Optimal resource allocation for MIMO ad hoc cognitive radio networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3117–3131, May 2011.

[37] O. El Ayach and R. W. Heath, Jr, "Grassmannian differential limited feedback for interference alignment," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6481–6494, Dec. 2012.

[38] R. T. Krishnamachari and M. K. Varanasi, "Interference alignment under limited feedback for MIMO interference channels," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3908–3917, Aug. 2013.

[39] N. Zhao, F. R. Yu, H. Sun, H. Yin, A. Nallanathan, and G. Wang, "Interference alignment with delayed channel state information and dynamic AR-model channel prediction in wireless networks," *Wireless Netw.*, vol. 21, no. 4, pp. 1227–1242, May 2015.

[40] L. Wu and W. Zhang, "Caching-based scalable video transmission over cellular networks," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1156–1159, Jun. 2016.